CLAIMS

1. A method of detecting a buffer overflow attack, the method comprising:

(a) detecting an address indicated by a return instruction when a processor return instruction is fetched;

(b) determining whether or not the detected address is in a stack area of the processor; and

(c) determining that the return instruction is illegal and a buffer overflow attack is made if the detected address is in the stack area.

2. The method of claim 1, wherein, in (c), the return instruction determined to be illegal is not executed and is discarded.

3. An apparatus for detecting a buffer overflow attack, the apparatus comprising:

an address detecting unit detecting an address indicated by a return instruction when a processor return instruction is fetched;

a confirmation unit determining whether or not the address detected by the address detecting unit is in a stack area of a processor; and

an attack determination unit determining that the return instruction is illegal and a buffer overflow attack is made if it is determined that the address detected by the address detecting unit is in the stack area.

4. The apparatus of claim 3, wherein the attack determination unit ignores the return instruction determined to be illegal so that the return instruction is not executed any longer.

5. A method of detecting a buffer overflow attack, the method comprising:

(a) detecting a return address returned to after a predetermined store instruction is executed;

(b) determining whether or not consecutive store instructions in a stack area of a processor modify the return address; and

(c) determining that a buffer overflow attack is made if it is determined that the consecutive store instructions modify the return address.

6. The method of claim 5, wherein, in (a), the return address returned to after the predetermined store instruction is executed is stored in a predetermined stack, and in (b), it is determined whether the return address is violated and modified by determining whether the address range of the consecutive store instructions overlaps with the return address stored in the stack.

7. An apparatus for detecting a buffer overflow attack, the apparatus comprising:

an address detecting unit detecting a return address returned to after a predetermined store instruction is executed;

an address modification determination unit determining whether or not consecutive store instructions in a stack area of a processor modify the return address detected by the address detecting unit; and

an attack determination unit determining that a buffer overflow attack is made if it is determined in the address modification determination unit that the consecutive store instructions modify the return address.

8. The apparatus of claim 7, wherein the address detecting unit stores in a predetermined stack the return address returned to after the predetermined store instruction is executed, and the address modification determination unit determines that the return address is violated and modified by determining whether or not the address range of the consecutive store instructions overlaps with the return address stored in the predetermined stack.

9. A method of recovering an operation state of a processor from a buffer overflow attack, the method comprising:

(a) detecting whether a buffer overflow attack is made on any write operation while storing write operations that are potential targets of buffer overflow attacks in a predetermined location instead of an original destination to store write operations;

(b) storing the contents stored in the predetermined location at a predetermined

interval in the original destination for storing write operations if no buffer overflow attack is detected and discarding unsafe write operations subsequent to a buffer overflow attack if a buffer overflow attack is detected; and

(c) ignoring the unsafe write operations subsequent to the buffer overflow attack if a buffer overflow attack is detected.

10. The method of claim 9, wherein, in (b), if a buffer overflow attack is detected, write operations stored before the buffer overflow attack is made are stored in the original destination for storing the write operations.

11. The method of claim 9, wherein, in (a), if there are second sets of consecutive write operations in contiguous regions of the original destination for storing write operations, the write operations are stored in the predetermined location, and otherwise the write operations are written to the original destination.

12. The method of claim 9, wherein if the original destination storing the write operations is accessed for a read operation, the original destination and the predetermined location storing the write operations are simultaneously accessed, and if an address for the read operation is included in the predetermined location storing the write operations, which are not yet stored in the original destination, data for the read operation is provided from the predetermined location storing the write operations.

13. An apparatus for recovering an operation state of a processor from a buffer overflow attack, the apparatus comprising:

a storing unit storing write operations that are potential targets of buffer overflow attacks in a predetermined storage unit, which is not a memory unit originally designated to store write operations;

an attack detecting unit detecting whether or not a buffer overflow attack is made on any of the write operations;

a storage management unit storing the contents stored in the predetermined storage unit in a memory unit which is originally designated to store write operations at a predetermined interval if no buffer overflow attack is detected and discarding unsafe

write operations subsequent to a buffer overflow attack if a buffer overflow attack is detected; and

a write management unit ignoring the unsafe write operations subsequent to the buffer overflow attack and not storing the unsafe write operations in the predetermined storage unit if a buffer overflow attack is detected.

14. The apparatus of claim 13, wherein the storage management unit stores write operations stored before the buffer overflow attack is made in the memory unit which is originally designated to store write operations if a buffer overflow attack is detected.

15. The apparatus of claim 13, wherein the storing unit stores the write operations in the predetermined storage unit if there are second sets of consecutive write operations in contiguous regions of the memory unit, which is originally designated to store write operations, and otherwise writes the write operations to the memory unit.

16. The apparatus of claim 13, further comprising:

a fetch management unit managing a read operation in the memory unit which is originally designated to store write operations,

wherein if there is a read operation in the memory unit which is originally designated to store write operations, the fetch management unit simultaneously accesses the memory unit and the predetermined storage unit in which data is stored by the storing unit, and if an destination address for the read operation is in the predetermined storage unit, not in the memory unit yet, data for the read operation is provided from the predetermined storage unit.

17. The apparatus of any one of claims 13 through 16, wherein the predetermined storage unit in which data are stored by the storing unit is a FIFO (first-in-first-out) device.

18. The apparatus of claim 17, wherein the predetermined interval at which the storage management unit stores the contents stored in the FIFO device in the

memory unit which is originally designated to store the write operations is determined according to the capacity of the FIFO device.